Abstract

There are many risks of network attacks under the Internet environment.

Internet Security is a vital issue and therefore, the intrusion detection is one major

research problem for business and personal networks to resist external attacks.

A Network Intrusion Detection System (NIDS) is a software application that

monitors the network or system activities for malicious activities and

unauthorized access to devices. The goal of designing a NIDS is to protect data’s

confidentiality and integrity. Our project focuses on these issues with the help of

Machine Learning. This project includes the implementation of different

machine learning algorithms including Linear regression, K-Means Clustering

and Artificial Neural Networks to automatically generate the rules for classify

network activities. A comparative analysis of these techniques to detect

intrusions has also been made. To learn the patterns of the attacks, NSL-KDD

dataset has been used.